UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,777	09/28/2001	David A. Lee	42390P11152	5083

7590 04/05/2005

BLAKELY, SOKOLOFF,
TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER	
SCHUBERT, KEVIN R	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 04/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/966,777	LEE, DAVID A.	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 September 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 September 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *09282001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-45 have been considered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-4,7-12,15,18-22,25-31,34-39,42, and 45 are rejected under 35 U.S.C. 102(b) as being anticipated by Richards, U.S. Patent No. 6,069,957.

As per claims 1,10,15,19,28,37, and 42, the applicant describes a method comprising the following limitations which are met by Richards:

a) generating a list of update keys on a key distribution center system based on a table of secret keys identifying valid and invalid receivers of a plurality of receivers, said list of update keys allowing valid receivers to decrypt a valid content key using update keys obtained from the list of update keys (Col 4, lines 52-67; Col 9, lines 12-31);

b) generating a multiple nested list of decryption patterns based on the list of update keys (Col 9, lines 12-31);

c) broadcasting said multiple nested list of decryption patterns to the plurality of receivers (Col 1, lines 25-31);

d) recovering a content key from the list of update keys by recovering a set of update keys for each receiver from the multiple nested list of decryption patterns and using the set of update keys to decrypt the content key (Col 9, lines 12-31);

Regarding part a), the key distribution center maintains a list or table of all the secret customer keys. The table identifies valid and invalid receivers because the valid receivers have a secret customer key in the table and the invalid receivers are the ones that are not reflected in the table.

As per claims 2,11,20,29, and 38, the applicant describes the method of claims 1,10,19,28, and 37, which are met by Richards (see above), with the following limitation which is also met by Richards:

Wherein generating a list of update keys comprises generating at least one intermediate key and one content key (Col 9, lines 12-31);

The intermediate keys are the CUSTOMER_CODE, which is the unique secret key of the customers maintained in the table of valid receivers, and the PK. The content key is the SK.

As per claims 3,12,21,30, and 39, the applicant describes the method of claims 2,11,20,29, and 38, which are met by Richards (see above), with the following limitation which is also met by Richards:

Wherein said generating at least one intermediate key and one content key comprises randomly generating said at least one intermediate key and one content key (Col 13, lines 48-49).

As per claims 4,22, and 31, the applicant describes the method of claims 3,21, and 30, which are met by Richards (see above), with the following limitation which is also met by Richards:

Wherein authorized receivers will receive an intermediate key that allows recovery of a valid content key and unauthorized receivers will receive an intermediate key that does not allow recovery of a valid content key (Col 14, lines 39-49);

In a second embodiment of the invention (Col 11, lines 14-22) which is similar to the embodiment described in the rejection for claim 1, Richards discloses that the intermediate key CAK can be changed according to such things like billing practices. Those who have the valid updated CAK intermediate key will be able to get to the content key, SK, while those who do not have the valid updated CAK (such as those who haven't paid their bill) have an intermediate key which does not allow the recovery of the content key, SK.

As per claims 7,18,25,34, and 45, the applicant describes the method of claims 1,15,19,28, and 42, which are met by Richards (see above), with the following limitation which is also met by Richards:

Wherein said recovering a set of update keys for each receiver from the multiple nested list of decryption patterns comprises parsing said multiple nested list of decryption patterns to locate an entry intended for a particular receiver based on detection of a predetermined test pattern included in an entry in the multiple nested list of decryption patterns (Col 9, lines 63-67);

The applicant discloses that "the purpose of the test pattern is to enable the receivers to locate keys intended for that receiver within the list of keys" (Applicant: page 11). The predetermined test pattern is therefore included to alert the receiver of how to decode and parse the incoming data with regard to the levels of encryption and the various keys used to encrypt the data for the receiver. Richards discloses that a header, or predetermined test pattern, alerts the receiver that the packet is a code packet and tells the receiver how to handle it.

As per claims 8,26, and 35, the applicant describes the method of claims 1,19, and 28, which are met by Richards (see above), with the following limitation which is also met by Richards:

Further comprising broadcasting content encrypted with said content key (Col 9, lines 26-31).

As per claims 9,27, and 36, the applicant describes the method of claims 8,26, and 35, which are met by Richards (see above), with the following additional limitation which is also met by Richards:

Further comprising decrypting said content encrypted with said content key using a content key recovered from the multiple nested list of decryption patterns (Col 9, lines 26-31).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5-6,13-14,16-17,23-24,32-33,40-41,43-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Richards in view of Uz, U.S. Patent No. 6,351,538.

As per claims 5,13,16,23,32,40, and 43, the applicant describes the method of claims 1,10,19,28,37, and 42, which are met by Richards (see above), with the following limitation which is met by Uz:

Wherein said generating a multiple nested list of decryption patterns comprises encrypting an entry of the list of update keys using a key that is a combination of a previous update key, a secret key for a receiver associated with the entry of the list of update keys, and an index indicating a location in said table of secret keys associated with each entry (Uz: Col 8, lines 25-31; Richards: Col 9, lines 12-31);

Richards discloses all the limitations of claims 1,10,19,28,37, and 42. Richards also discloses encrypting an entry of the list of update keys using a key that is a combination of a previous update key and a secret key for a receiver associated with the entry of the list of update keys. This is done because the content key, SK, is an encryption of a previous update key, PK, and a secret key for a receiver associated with the entry of the list of update keys, CUSTOMER_CODE.

Richards fails to disclose an "index indicating a location in said table of secret keys associated with each entry". Uz discloses a one way broadcasting system which broadcasts key and content information for conditional access systems, such as a pay-per-view system. Uz system also discloses the use of maintaining key tables. Furthermore, Uz discloses the idea of transmitting an index indicating a location in the table of secret keys which can be used to locate keys for decryption.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Uz with those of Richards and incorporate the use of an index indicating a location in a table of secret keys so that the receiver can use the index to locate secret keys for decryption.

As per claims 6,14,17,24,33,41, and 44, the applicant describes the method of claims 5,13,16,23,32,40, and 43, which are met by Richards (see above), with the following additional limitation which is met by Uz:

Wherein an entry in said multiple nested list of decryption patterns includes a predetermined test pattern encrypted with the secret keys for a receiver associated with the entry of the list of update keys (Col 9, lines 63-67);

Richards discloses all the limitations of claims 5,13,16,23,32,40, and 43. However Richards fails to disclose the use of encrypting the predetermined test pattern with the secret keys for a receiver. As discussed in the rejection for claim 7, the predetermined test pattern which provides decryption instructions for the receiver corresponds to the header of Richards' system which, like the predetermined test pattern, provides decryption instructions. In short, Richards' system discloses all the limitations of the above claim except for the limitation of encrypting the header information.

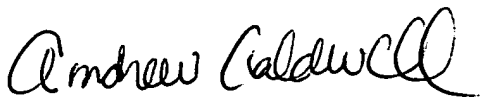
Uz discloses a one way broadcasting system which broadcasts key and content information for conditional access systems, such as a pay-per-view system. Furthermore, Uz discloses the idea of encrypting header information (Col 6, lines 13-14).

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Uz and Richards and encrypt the header of information of Richards' system because doing so would make the system more secure and less vulnerable to hackers being able to intercept the broadcast and know information about the data.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



***

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER